UDC 004.056.57

Machine Learning for APT Detection in Industrial IoT

Hajjouz A. (ИТМО University)
Scientific director – associate professor, Avksenteva E.Y. (ИТМО University)

Introduction. The security of the Industrial Internet of Things (IIoT) has become paramount due to the increasing cyberattacks targeting critical infrastructure. This study aims to develop an effective framework for detecting Advanced Persistent Threats (APTs) in IIoT environments by leveraging machine learning techniques and a new dataset specifically designed for this purpose.

Main part. The study utilizes the CIC APT IIoT 2024 dataset [1], a specialized dataset that includes network logs and provenance data to track the different stages of attacks. The CatBoost algorithm, a powerful machine learning algorithm, was used to achieve unprecedented precision and recall in detecting APTs. The study also included a hierarchical feature selection process to reduce complexity, enhance model interpretability, and process data in real-time [2].

The results showed that the CatBoost algorithm is capable of detecting sophisticated APT attacks with high accuracy and reduced false alarms. In addition, the most important features that contributed to the model's accuracy were analyzed, such as Timestamp (ts), Destination Port, Source Port, Syn Count, Urg Count, and Flow Duration.

The model was tested to ensure its ability to detect APTs in real-time and demonstrated good performance, with an average processing speed of 1,600,596.84 samples per second..

Conclusions. This study presents an effective framework for detecting APTs in IIoT environments using the CatBoost algorithm and the CIC APT IIoT 2024 dataset. This work contributes to the development of specialized security solutions for IIoT and provides a basis for future research in this field.

List of sources used:

1. Ghiasvand, E., Ray, S., Iqbal, S., Dadkhah, S., & Ghorbani, A. A. (2024). CICAPT-IIOT: A provenance-based APT attack dataset for IIoT environment. arXiv preprint arXiv:2407.11278.
2. Hajjouz, A., & Avksentieva, E. . (2024). Optimizing Intrusion Detection for DoS, DDoS, and Mirai Attacks Subtypes Using Hierarchical Feature Selection and CatBoost on the CICIoT2023 Dataset. Data and Metadata, 3, 577.